



WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE
INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

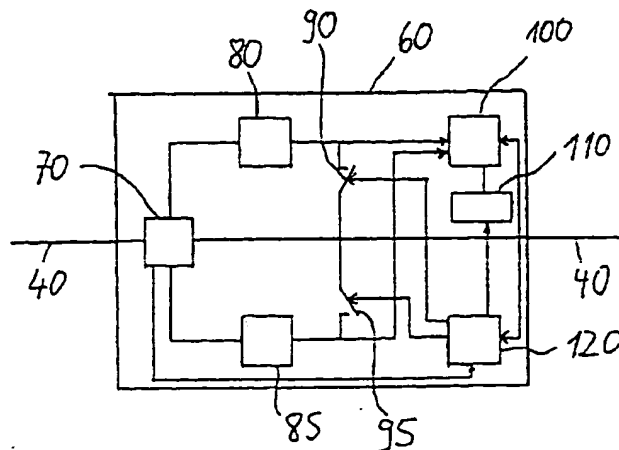
(51) Internationale Patentklassifikation ⁶ : H04Q 11/04	A2	(11) Internationale Veröffentlichungsnummer: WO 98/53635
(21) Internationales Aktenzeichen: PCT/EP98/02121		(43) Internationales Veröffentlichungsdatum: 26. November 1998 (26.11.98)
(22) Internationales Anmeldedatum: 11. April 1998 (11.04.98)		(81) Bestimmungsstaaten: CA, CN, JP, KR, TR, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).
(30) Prioritätsdaten: 197 20 719.7 16. Mai 1997 (16.05.97) DE		Veröffentlicht <i>Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.</i>
(71) Anmelder (für alle Bestimmungsstaaten ausser US): DEUTSCHE TELEKOM AG [DE/DE]; Friedrich-Ebert-Allee 140, D-53113 Bonn (DE).		
(72) Erfinder; und (75) Erfinder/Anmelder (nur für US): STOLZ, Helmut [DE/DE]; Am Gensberge 12, D-57080 Siegen (DE).		

(54) Title: DEVICE FOR MONITORING A CONNECTION SETUP

(54) Bezeichnung: VERBINDUNGS-AUFBAU-ÜBERWACHUNGSVORRICHTUNG

(57) Abstract

The invention relates to a device for protecting a data terminal, specially a personal computer, connected to a digital communication network against unauthorized external access. To this end, the device (60) is interposed between at least one data terminal (20, 30) and a network terminal (50), which are connected via a terminal end connection (40). At least one storage device (80, 85) is provided for the intermediate storage of a call number transmitted by the data terminal (20, 30) via a control channel. At least one predetermined call number is filed in a second storage device (110). A comparator compares the call number stored in the intermediate memory with each of the predetermined stored call numbers. In case of positive comparison results, the device transmits the call number stored in the intermediate storage to the network terminal or blocks the transmission of the call number in case of negative comparison results thereby impeding connection to a hacker.



BEST AVAILABLE COPY

(57) Zusammenfassung

Die Erfindung betrifft eine Vorrichtung zum Schutz einer an ein digitales Kommunikationsnetz angeschalteten Dateneneinrichtung, insbesondere eines Personal-Computers, gegen unberechtigte externe Zugriffe. Dazu ist die Vorrichtung (60) zwischen wenigstens eine Dateneneinrichtung (20, 30) und eine Netzabschlußeinrichtung (50) zwischengeschaltet, die über eine Endeinrichtungs-Anschlußleitung (40) verbunden sind. Wenigstens eine erste Speichereinrichtung (80, 85) ist vorgesehen, um eine von der Dateneneinrichtung (20, 30) über einen Steuerkanal übertragene Rufnummer zwischenzuspeichern. In einer zweiten Speichereinrichtung (110) ist wenigstens eine vorbestimmte Rufnummer abgelegt. Eine Vergleichseinrichtung vergleicht die zwischengespeicherte Rufnummer mit jeder gespeicherten vorbestimmten Rufnummer. In Abhängigkeit von einem positiven Vergleichsergebnis leitet eine Einrichtung die zwischengespeicherte Rufnummer zur Netzabschlußeinrichtung weiter oder sperrt in Abhängigkeit von einem negativen Vergleichsergebnis die Weitergabe der Rufnummer und verhindert damit einen Verbindungsaufbau zu einem Eindringling.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäß dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland	ML	Mali	TR	Türkei
BG	Bulgarien	HU	Ungarn	MN	Mongolei	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MR	Mauritanien	UA	Ukraine
BR	Brasilien	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Island	MX	Mexiko	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	NE	Niger	UZ	Usbekistan
CF	Zentralafrikanische Republik	JP	Japan	NL	Niederlande	VN	Vietnam
CG	Kongo	KE	Kenia	NO	Norwegen	YU	Jugoslawien
CH	Schweiz	KG	Kirgisistan	NZ	Neuseeland	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	PL	Polen		
CM	Kamerun	KR	Republik Korea	PT	Portugal		
CN	China	KZ	Kasachstan	RO	Rumänien		
CU	Kuba	LC	St. Lucia	RU	Russische Föderation		
CZ	Tschechische Republik	LI	Liechtenstein	SD	Sudan		
DE	Deutschland	LK	Sri Lanka	SE	Schweden		
DK	Dänemark	LR	Liberia	SG	Singapur		
EE	Estland						

zischengespeicherte Rufnummer mit allen in der zweiten Speichereinrichtung gespeicherten Rufnummern vergleichen muß.

Wird der Steuereinrichtung von der Vergleichseinrichtung signalisiert, daß die zischengespeicherte Rufnummer mit einer der in der zweiten Speichereinrichtung gespeicherten Rufnummer übereinstimmt, deaktiviert sie den Steuerkanal-Decoder, so daß nach einem Verbindungsaufbau die Endeinrichtungs-Anschlußleitung von der angeschalteten Datenendeinrichtung durch das Verbindungsaufbau-Überwachungsgerät zur Netzabschlußeinrichtung durchgeschaltet ist.

Die erste Speichereinrichtung zur Zwischenspeicherung einer zu rufenden Rufnummer ist zweckmäßigerweise ein Schieberegister, in das die Rufnummer seriell eingetaktet wird.

Gemäß einem Ausführungsbeispiel weist die Netzabschlußeinrichtung eine ISDN-Anschlußkonfiguration mit einer S_0 -Schnittstelle auf. Die ISDN-Anschlußkonfiguration kann für einen Basisanschluß umfassend zwei Nutzkanäle und einen Steuerkanal oder einen Primärmultiplexanschluß umfassend 30 Nutzkanäle und einen Steuerkanal ausgelegt sein. Bei der Endeinrichtungs-Anschlußleitung handelt es sich in diesem Fall um einen S_0 -Bus, wobei der Steuerkanal der D-Kanal ist.

Das Verbindungsaufbau-Überwachungsgerät kann eine Tastatur zur Eingabe der vorbestimmten Rufnummern in die zweite Speichereinrichtung aufweisen. Ergänzend oder alternativ kann eine Schnittstelle zum Anschalten eines Computers vorgesehen sein, über den die Steuereinrichtung programmierbar ist und die vorbestimmten Rufnummern für die jeweiligen Datenendeinrichtungen eingegeben werden können.

Falls ein externer Angriff auf eine angeschaltete Datenendeinrichtung erfolgt, ist eine Einrichtung zur optischen und/oder akustischen Signalisierung eines Verbindungsabbruchs vorgesehen.

Anstatt das Verbindungsaufbau-Überwachungsgeräts als separate Einheit in die Endeinrichtungs-Anschlußleitung

einzuschleifen, ist es denkbar, das Gerät in der Netzabschlußeinrichtung anzuordnen.

Die Erfindung wird nachfolgend anhand eines Ausführungsbeispiels in Verbindung mit den beiliegenden Zeichnungen näher erläutert. Es zeigen:

Fig. 1 ein stark vereinfachtes Blockschaltbild eines ISDN-Netzes, an das beispielsweise zwei Endeinrichtungen angeschlossen sind, und

Fig. 2 das in Fig. 1 dargestellte, erfindungsgemäße Verbindungsaufbau-Überwachungsgerät.

Fig. 1 zeigt schematisch dargestellt ein ISDN-Netz 10, an das zwei Datenendeeinrichtungen, in unserem Beispiel zwei Personal-Computer 20 und 30, über einen S₀-Bus 40 und über eine Netzabschlußeinrichtung 50 angeschlossen sind. Für unser Beispiel sei angenommen, daß die Netzabschlußeinrichtung 50 für einen ISDN-Basisanschluß umfassend zwei B-Kanäle (Nutzkanäle) und einen D-Kanal (Steuerkanal) ausgebildet ist. Es sei darauf hingewiesen, daß die Erfindung in jedem digitalen Kommunikationsnetz Anwendung finden kann, in dem Verbindungsaufbauinformationen über einen getrennten Steuerkanal übertragen werden. Jeder Personal-Computer 20, 30 ist mit einer ISDN-Schnittstellenkarte versehen, über die er an den S₀-Bus 40 angeschlossen ist. Der hier benutzte S₀-Bus 40 kann mit maximal acht Endeeinrichtungen verbunden sein. Falls in einer oder beiden ISDN-Schnittstellenkarten der jeweiligen Computer 20 und 30 ein sogenanntes Trojanisches Pferd implementiert ist, können die befallenen Computer 20 und 30 veranlaßt werden, zu einem Angreifer eine Verbindung aufzubauen, über die der Angreifer unmittelbar in die Personal-Computer 20 und 30 eindringen kann. Um einen solchen Angriff zu vermeiden, ist teilnehmerseitig in den S₀-Bus 40 zwischen den Personal-Computern 20 und 30 und der Netzabschlußeinrichtung 50 ein Verbindungsaufbau-Überwachungsgerät 60 eingeschleift. Wie nachfolgend noch ausführlicher erläutert wird, dient das Verbindungsaufbau-Überwachungsgerät 60 dazu, den Aufbau einer Verbindung nur zu vorbestimmten Teilnehmern zuzulassen.

Verbindungsaufbau-Überwachungsvorrichtung

Die Erfindung handelt von einer Vorrichtung zum Schutz einer an ein digitales Kommunikationsnetz angeschalteten Datenendeinrichtung, insbesondere eines Personal Computers, gegen unberechtigte externe Zugriffe.

Datenendgeräte, wie z. B. Faxgeräte oder Personal Computer, sind teilnehmerseitig mittels einer eingesteckten ISDN-Schnittstellenkarte an den S₀-Bus einer ISDN-Anschlußkonfiguration angeschaltet. Es sind heutzutage Angriffsszenarien bekannt, bei denen während der Herstellung von solchen ISDN-Schnittstellenkarten in die jeweilige Kommunikations-Anwendungsschnittstelle sogenannte "Viren" oder "Trojanische Pferde" implementiert werden. Solche "Trojanischen Pferde" enthalten die Rufnummer eines Eindringlings und sind in der Lage, von dem befallenen Datenendgerät aus einen Verbindungsaufbau zu dem Eindringling aufzubauen, der danach unmittelbaren Zugriff zu Datenbeständen und Anwendungsprogrammen des befallenen Datenendgeräts hat.

Der Erfindung liegt daher die Aufgabe zugrunde, eine Vorrichtung zu schaffen, mit der an ein digitales Kommunikationsnetz angeschaltete Datenendeinrichtungen gegen unberechtigte externe Zugriffe geschützt werden können.

Dieses technische Problem löst die Erfindung mit den Merkmalen des Anspruchs 1. Vorteilhafte Weiterbildungen sind in den Unteransprüchen angegeben.

Um einen unberechtigten externen Zugriff auf eine an ein digitales Kommunikationsnetz angeschaltete Datenendeinrichtung zu verhindern, ist eine Vorrichtung, im Nachfolgenden "Verbindungsaufbau-Überwachungsgerät" genannt, zwischen wenigstens eine Datenendeinrichtung und eine Netzabschlußeinrichtung, die über eine Endeinrichtungs-Anschlußleitung verbunden sind, zwischengeschaltet. Das Verbindungsaufbau-Überwachungsgerät enthält wenigstens eine erste Speichereinrichtung zum Zwischenspeichern einer von der Datenendeinrichtung über

2

einen Steuerkanal übertragenen Rufnummer. Darüber hinaus ist eine zweite Speichereinrichtung vorgesehen, in der wenigstens eine vorbestimmte Rufnummer ablegbar ist. Eine Vergleichseinrichtung dient dazu, die zwischengespeicherte Rufnummer mit jeder vorbestimmten gespeicherten Rufnummer zu vergleichen. Ferner enthält das Verbindungsaufbau-Überwachungsgerät eine Einrichtung, die in Abhängigkeit von einem positiven Vergleichsergebnis der Vergleichseinrichtung die zwischengespeicherte Rufnummer zur Netzabschlußeinrichtung weiterleitet und in Abhängigkeit von einem negativen Vergleichsergebnis die Weitergabe der Rufnummer sperrt und damit einen Verbindungsaufbau zu einem der Rufnummer zugeordneten Teilnehmer verhindert.

Sind mehrere Datenendeinrichtungen an die Endeinrichtungs-Anschlußleitung angeschlossen, so ist in der zweiten Speichereinrichtung für jede Datenendeinrichtung wenigstens eine vorbestimmte Rufnummer abgespeichert. Auf diese Weise kann jede angeschaltete Datenendeinrichtung nur zu dem Teilnehmer eine Verbindung aufbauen, dessen Rufnummer in der zweiten Speichereinrichtung abgelegt ist.

Das Verbindungsaufbau-Überwachungsgerät weist ferner eine Steuereinrichtung auf, die zweckmäßigerweise bei einem negativen Vergleichsergebnis die zwischengespeicherte Rufnummer aus der ersten Speichereinrichtung löscht.

Teilnehmerseitig ist in dem Verbindungsaufbau-Überwachungsgerät ein Steuerkanal-Decoder vorgesehen, der die von der rufenden Datenendeinrichtung übertragene Verbindungsaufbauinformation empfängt und daraus die Rufnummer und die Identifikationsnummer der rufenden Datenendeinrichtung gewinnt.

Die Steuereinrichtung ist derart programmiert, daß sie unter Ansprechen auf die vom Steuerkanal-Decoder erhaltene Identifikationsnummer nur die in der zweiten Speichereinrichtung gespeicherten Rufnummern an die Vergleichseinrichtung anlegt, die der entsprechenden Datenendeinrichtung zugeordnet sind. Auf diese Weise wird verhindert, daß die Vergleichseinrichtung die

Fig. 2 zeigt ein mögliches Blockschaltbild zur schaltungstechnischen Realisierung des Verbindungsaufbau-Überwachungsgerätes 60. Teilnehmerseitig weist das Verbindungsaufbau-Überwachungsgerät einen Steuerkanal-Decoder, in unserem Beispiel einen D-Kanal-Decoder 70, auf.

Der D-Kanal-Steuerkanal-Decoder 70 hat die Aufgabe, die von den Personal-Computern 20 und 30 kommenden Verbindungsaufbau-Informationen zu empfangen und daraus die gewünschte Rufnummer sowie die den jeweiligen Personal-Computer kennzeichnende Identifikationsnummer zu gewinnen. Da der hier benutzte ISDN-Basisanschluß über zwei B-Kanäle verfügt, können die beiden Personal-Computer 20 und 30 gleichzeitig mit verschiedenen Teilnehmern kommunizieren. Aus diesem Grund ist der D-Kanal-Decoder 70 ausgangsseitig mit zwei Speichereinrichtungen 80, 85 verbunden. Die Speichereinrichtungen 80, 85 können als Schieberegister ausgebildet sein. Eingangsseitig ist der D-Kanal-Decoder mit dem S_0 -Bus 40 verbunden. Der S_0 -Bus 40 verläßt ausgangsseitig den D-Steuerkanal-Decoder 70 und führt an den Eingang der Netzabschlußeinrichtung 50. Jedes Schieberegister 80, 85 ist beispielsweise über einen Schalter 90 bzw. 95 mit dem S_0 -Bus 40 am Ausgang des D-Steuerkanal-Decoders 70 verbunden. Der D-Steuerkanal-Decoder 70 filtert, wie bereits erwähnt, aus der Verbindungsaufbauinformation die Rufnummer aus und schiebt sie in eines der Schieberegister 80, 85 ein. Der Ausgang der Schieberegister 80, 85 ist jeweils eingangsseitig mit einer Vergleichseinrichtung 100 verbunden. An einen weiteren Eingang der Vergleichseinrichtung 100 ist eine Speichereinrichtung 110 angeschlossen, in der für jeden Personal-Computer 20 und 30 vorbestimmte Rufnummern abgelegt sind. Eine Steuereinrichtung 120 ist eingangsseitig mit einem Ausgang des D-Steuerkanal-Decoders 70 verbunden und empfängt von dem D-Steuerkanal-Decoder 70 die Identifikationsnummer des jeweils rufenden Personal-Computers 20 und/oder 30. Ferner ist die Steuereinrichtung 120 mit den beiden Schaltern 90 und 95, der Speichereinrichtung 110 und der Vergleichseinrichtung 100 verbunden. Das

Verbindungsaufbau-Überwachungsgerät 60 kann ferner eine Tastatur aufweisen, über die die vorbestimmten Rufnummern für die Personal-Computer 20 und 30 in die Speichereinrichtung 110 eingegeben werden können. Alternativ oder ergänzend kann das Verbindungsaufbau-Überwachungsgerät 60 eine Schnittstelle aufweisen, an die ein Computer (nicht dargestellt) angeschlossen sein kann. Mit Hilfe des Computers können beispielsweise vorbestimmte Rufnummern in die Speichereinrichtung 110 eingeschrieben werden. Die Steuereinrichtung 120 ist auch mit einer optischen und/oder akustischen Warneinrichtung (nicht dargestellt) verbunden. Die Warneinrichtung wird von der Steuereinrichtung 120 aktiviert, einen Verbindungsabbruch zu signalisieren, wenn die Vergleichseinrichtung 100 feststellt, daß die im Schieberegister 80 und/oder 85 zwischengespeicherte Rufnummer nicht mit einer der in der Speichereinrichtung 110 abgelegten Rufnummer übereinstimmt. Beispielsweise kann das Warnsignal über den D-Kanal des S₀-Busses 40 zum Personal-Computer 20, 30 gesendet werden und dort ein optisches oder akustisches Warnsignal auslösen. Obwohl das erfindungsgemäße Verbindungsaufbau-Überwachungsgerät 60 als separate Einrichtung beschrieben ist, kann es in der Netzabschlußeinrichtung 50 selbst angeordnet sein. Die Speisung des Verbindungsaufbau-Überwachungsgeräts 60 erfolgt beispielsweise über eine eigene Stromversorgungseinrichtung (nicht dargestellt).

Es wird nunmehr die Funktionsweise des erfindungsgemäßen Verbindungsaufbau-Überwachungsgeräts 60 erläutert. Es sei angenommen, daß in der Speichereinrichtung 110 für den Personal-Computer 20 zwei Rufnummern, beispielsweise die Rufnummern 1010 und 1111, und für den Personal-Computer 30 ebenfalls zwei Rufnummern, beispielsweise die Rufnummern 1000 und 0001, abgelegt sind. Im Anfangszustand seien ferner die Schalter 90 und 95 geöffnet. Wir gehen zunächst davon aus, daß der Personal-Computer 20 einen Verbindungsaufbau zu einem Teilnehmer mit der Rufnummer 1111 einleiten möchte. Dazu sendet er über den D-Kanal des S₀-Busses 40 in einem

festgelegten Protokoll die Rufnummer 1111 zum ISDN-Netz 10. Die vom Personal-Computer 20 ausgesendete Verbindungsaufbauinformation, die sowohl die Rufnummer 1111 als auch seine Identifikationsnummer enthält, wird zum D-Kanal-Decoder 70 des Verbindungsaufbau-Überwachungsgerätes 60 übertragen. Der D-Kanal-Decoder 70 leitet aus der Verbindungsaufbauinformation die Identifikationsnummer ab und überträgt sie zur Steuereinrichtung 120. Die Steuereinrichtung 120 sorgt dafür, daß die beiden in der Speichereinrichtung 110 für den Personal-Computer 20 gespeicherten Rufnummern 1111 und 1010 nacheinander an die Vergleichseinrichtung 100 angelegt werden. Der D-Kanal-Decoder 70 leitet außerdem aus den empfangenen Verbindungsaufbauinformationen die Rufnummer 1111 ab und leitet sie an das Schieberegister 80 weiter. Anschließend wird die zwischengespeicherte Rufnummer des Schieberegisters 80 an die Vergleichseinrichtung 100 angelegt und nacheinander mit den beiden Rufnummern, die von dem Speicherregister 110 angelegt werden, verglichen. Die Vergleichseinrichtung 100 signalisiert der Steuereinrichtung 120, daß die zwischengespeicherte Rufnummer mit einer der beiden vorbestimmten Rufnummern übereinstimmt, die dem Personal-Computer 20 zugeordnet sind. Daraufhin schließt die Steuereinrichtung 120 den Schalter 90, und das Schieberegister 80 schiebt die gespeicherte Rufnummer 1111 auf den S₀-Bus 40. Die akzeptierte Rufnummer wird über die Netzabschlußeinrichtung 50 zu einer entsprechenden Vermittlungsstelle des ISDN-Netzes 10 übertragen, woraufhin eine Verbindung zwischen dem Personal-Computer 20 und dem gerufenen Teilnehmer mit der Rufnummer 1111 hergestellt wird. Nachdem die Rufnummer zum ISDN-Netz 10 übertragen worden ist, deaktiviert die Steuereinrichtung 120 den D-Kanal-Decoder 70 und öffnet wieder den Schalter 90. Auf diese Weise ist der Personal-Computer 20 unmittelbar über den S₀-Bus 40 mit der Netzabschlußeinrichtung 50 und mit dem gerufenen Teilnehmer verbunden. Jetzt können zwischen dem gerufenen Teilnehmer und dem Personal-Computer 20 Daten ausgetauscht werden.

Es sei ferner angenommen, daß auch der zweite Personal-Computer 30 einen Verbindungswunsch hat. Dazu sendet der Personal-Computer 30 seine Verbindungsaufbauinformationen zunächst zum D-Steuerkanal-Decoder 70. In unserem Beispiel enthält aber die ISDN-Schnittstellenkarte des Personal-Computers 30 ein Trojanisches Pferd, das diesen Verbindungsaufbauwunsch mit der Rufnummer 0110 einleiten möchte. Der D-Kanal-Decoder 70 filtert die Rufnummer aus der Verbindungsaufbauinformation heraus und schiebt sie in das Schieberegister 85. Ferner entnimmt der D-Kanal-Decoder 70 der Verbindungsaufbauinformationen die Identifikationsnummer des Personal-Computers 30 und leitet diese der Steuereinrichtung 120 zu. Die Steuereinrichtung 120 sorgt wiederum dafür, daß diesmal die beiden dem Personal-Computer 30 zugeordneten Rufnummern 0001 und 1000 aus der Speichereinrichtung 110 an die Vergleichseinrichtung 100 nacheinander angelegt werden. Die Vergleichseinrichtung 100 vergleicht nun nacheinander die in dem Schieberegister 85 zwischengespeicherte Rufnummer 0110 mit den zulässigen Rufnummern für den Personal-Computer 30. Da die Vergleichseinrichtung 100 keine Übereinstimmung zwischen den Rufnummern feststellt, bleibt der Schalter 95 geöffnet, und der Verbindungsaufbau wird damit abgebrochen. Gleichzeitig löscht die Steuereinrichtung 120 den Inhalt des Schieberegisters 85.

Darüber hinaus wird die nicht dargestellte optische und akustische Warneinrichtung aktiviert, um den Verbindungsabbruch und damit dem Teilnehmer einen externen Angriff auf den Personal-Computer 30 zu signalisieren.

Patentansprüche

1. Vorrichtung zum Schutz einer an ein digitales Kommunikationsnetz angeschalteten Datenendeinrichtung gegen unberechtigte externe Zugriffe, mit folgenden Merkmalen:
die Vorrichtung (60) ist zwischen wenigstens eine Datenendeinrichtung (20, 30) und eine Netzabschlußeinrichtung (50), die über eine Endeinrichtungs-Anschlußleitung (40) verbunden sind, zwischengeschaltet,
wenigstens eine erste Speichereinrichtung (80, 85) zum Zwischenspeichern einer von der Datenendeinrichtung (20, 30) über einen Steuerkanal übertragenen Rufnummer, eine zweite Speichereinrichtung (110), in der wenigstens eine vorbestimmte Rufnummer ablegbar ist, eine Vergleichseinrichtung (100), die die zwischengespeicherte Rufnummer mit jeder gespeicherten Rufnummer vergleicht, und
eine Einrichtung (120, 90, 95), die in Abhängigkeit von einem positiven Vergleichsergebnis die zwischengespeicherte Rufnummer zur Netzabschlußeinrichtung (50) weiterleitet oder in Abhängigkeit von einem negativen Vergleichsergebnis die Weitergabe der Rufnummer sperrt.
2. Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, daß in der zweiten Speichereinrichtung (110) für jede Datenendeinrichtung (20, 30) wenigstens eine vorbestimmte Rufnummer speicherbar ist.
3. Vorrichtung nach Anspruch 1 oder 2, gekennzeichnet durch eine Steuereinrichtung (120), die bei einem negativen Vergleichsergebnis die Rufnummer aus der ersten Speichereinrichtung (80, 85) löscht, und durch einen Steuerkanal-Decoder (70), der aus einer von der Datenendeinrichtung (20, 30) übertragenen Verbindungsaufbauinformation die Rufnummer und die

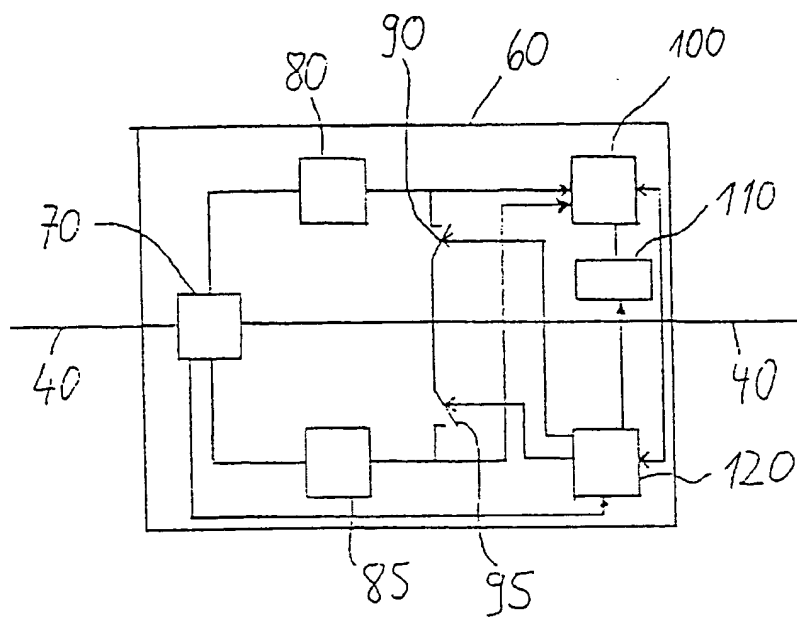
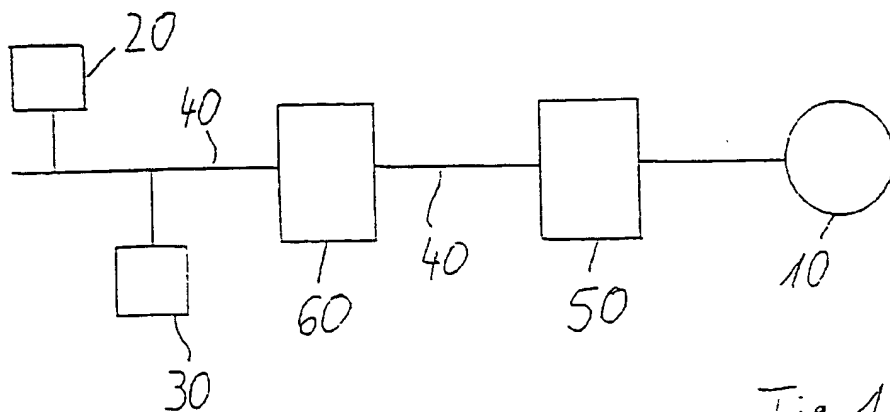
10

Identifikationsnummer der Datenendeinrichtung (20, 30) erhält.

4. Vorrichtung nach Anspruch 3, dadurch gekennzeichnet, daß die Steuereinrichtung (120) unter Ansprechen auf die vom Steuerkanal-Decoder (70) erhaltene Identifikationsnummer nur die in der zweiten Speichereinrichtung (110) gespeicherten Rufnummern an die Vergleichseinrichtung (100) anlegt, die der entsprechenden Datenendeinrichtung (20, 30) zugeordnet sind.
5. Vorrichtung nach Anspruch 3 oder 4, dadurch gekennzeichnet, daß die Steuereinrichtung (120) bei einem positiven Vergleichsergebnis den Steuerkanal-Decoder (70) deaktiviert.
6. Vorrichtung nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß die erste Speichereinrichtung (80, 85) ein Schieberegister ist.
7. Vorrichtung nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Netzabschlußeinrichtung (50) eine ISDN-Anschlußkonfiguration mit einer S₀-Schnittstelle aufweist, daß die Endeinrichtungs-Anschlußleitung (40) ein S₀-Bus ist, und daß der Steuerkanal der D-Kanal ist.
8. Vorrichtung nach einem der Ansprüche 1 bis 7, gekennzeichnet durch eine Tastatur zur Eingabe der vorbestimmten Rufnummern.
9. Vorrichtung nach einem der Ansprüche 1 bis 8, gekennzeichnet durch eine Schnittstelle zum Anschalten eines Computers.

10. Vorrichtung nach einem der Ansprüche 1 bis 9, gekennzeichnet durch eine Einrichtung zur optischen und/oder akustischen Signalisierung eines Verbindungsabbruchs bei einem negativen Vergleichsergebnis.
11. Vorrichtung nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, daß die Vorrichtung (60) in der Netzabschlußeinrichtung (50) integriert ist.
12. Vorrichtung nach einem der Ansprüche 1 bis 11, gekennzeichnet durch eine Energieversorgungseinrichtung.

1 / 1



PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales BüroINTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE
INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

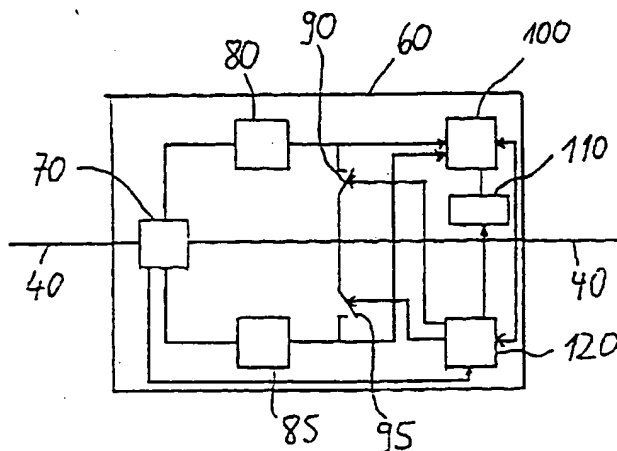
(51) Internationale Patentklassifikation ⁶ : H04Q 11/04	A3	(11) Internationale Veröffentlichungsnummer: WO 98/53635 (43) Internationales Veröffentlichungsdatum: 26. November 1998 (26.11.98)
(21) Internationales Aktenzeichen: PCT/EP98/02121 (22) Internationales Anmeldedatum: 11. April 1998 (11.04.98) (30) Prioritätsdaten: 197 20 719.7 16. Mai 1997 (16.05.97) DE (71) Anmelder (für alle Bestimmungsstaaten ausser US): DEUTSCHE TELEKOM AG [DE/DE]; Friedrich-Ebert-Allee 140, D-53113 Bonn (DE). (72) Erfinder; und (75) Erfinder/Anmelder (nur für US): STOLZ, Helmut [DE/DE]; Am Gensberge 12, D-57080 Siegen (DE).	(81) Bestimmungsstaaten: CA, CN, JP, KR, TR, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Veröffentlicht Mit internationalem Recherchenbericht. (88) Veröffentlichungsdatum des internationalen Recherchenbe- richts: 25. Februar 1999 (25.02.99)	

(54) Title: DEVICE FOR MONITORING A CONNECTION SETUP

(54) Bezeichnung: VERBINDUNGS-AUFBAU-ÜBERWACHUNGSVORRICHTUNG

(57) Abstract

The invention relates to a device for protecting a data terminal, specially a personal computer, connected to a digital communication network against unauthorized external access. To this end, the device (60) is interposed between at least one data terminal (20, 30) and a network terminal (50), which are connected via a terminal end connection (40). At least one storage device (80, 85) is provided for the intermediate storage of a call number transmitted by the data terminal (20, 30) via a control channel. At least one predetermined call number is filed in a second storage device (110). A comparator compares the call number stored in the intermediate memory with each of the predetermined stored call numbers. In case of positive comparison results, the device transmits the call number stored in the intermediate storage to the network terminal or blocks the transmission of the call number in case of negative comparison results thereby impeding connection to a hacker.



(57) Zusammenfassung

Die Erfindung betrifft eine Vorrichtung zum Schutz einer an ein digitales Kommunikationsnetz angeschalteten Datenendeinrichtung, insbesondere eines Personal-Computers, gegen unberechtigte externe Zugriffe. Dazu ist die Vorrichtung (60) zwischen wenigstens eine Datenendeinrichtung (20, 30) und eine Netzabschlußeinrichtung (50) zwischengeschaltet, die über eine Endeinrichtungs-Anschlußleitung (40) verbunden sind. Wenigstens eine erste Speichereinrichtung (80, 85) ist vorgesehen, um eine von der Datenendeinrichtung (20, 30) über einen Steuerkanal übertragene Rufnummer zwischenzuspeichern. In einer zweiten Speichereinrichtung (110) ist wenigstens eine vorbestimmte Rufnummer abgelegt. Eine Vergleichseinrichtung vergleicht die zwischengespeicherte Rufnummer mit jeder gespeicherten vorbestimmten Rufnummer. In Abhängigkeit von einem positiven Vergleichsergebnis leitet eine Einrichtung die zwischengespeicherte Rufnummer zur Netzabschlußeinrichtung weiter oder sperrt in Abhängigkeit von einem negativen Vergleichsergebnis die Weitergabe der Rufnummer und verhindert damit einen Verbindungsaufbau zu einem Eindringling.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäß dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenico
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Verinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MX	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland	ML	Mali	TR	Türkei
BG	Bulgarien	HU	Ungarn	MN	Mongolei	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MR	Mauritanien	UA	Ukraine
BR	Brasilien	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Island	MX	Mexiko	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	NE	Niger	UZ	Usbekistan
CF	Zentralafrikanische Republik	JP	Japan	NL	Niederlande	VN	Vietnam
CG	Kongo	KE	Kenia	NO	Norwegen	YU	Jugoslawien
CH	Schweiz	KG	Kirgisistan	NZ	Neuseeland	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	PL	Polen		
CM	Kamerun	KR	Republik Korea	PT	Portugal		
CN	China	KZ	Kasachstan	RO	Rumänien		
CU	Kuba	LC	St. Lucia	RU	Russische Föderation		
CZ	Tschechische Republik	LI	Liechtenstein	SD	Sudan		
DE	Deutschland	LK	Sri Lanka	SE	Schweden		
DK	Dänemark	LR	Liberia	SG	Singapur		
EE	Estland						

INTERNATIONAL SEARCH REPORT

International application No.

PCT/EP 98/02121

A. CLASSIFICATION OF SUBJECT MATTER		
IPC ⁶ : H 04 Q 11/04 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) IPC ⁶ : H 04 L, H 04 M, H 04 Q		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GB 2301264 A (MITSUBISHI DENKI KABUSHIKI KAISHA) 27 November 1996 (27.11.96), abstract, page 1, line 1 - page 10, line 13, fig. 5, claims 1,2	1
A	US 5369707 A (FOLLENDRE, III) 29 November 1994 (29.11.94), abstract, column 1, line 5 - column 4, line 15, fig. 4, claim 1.	1
A	US 5548635 A (BRADLEY et al.) 20 August 1996 (20.08.96)	
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
<p>* Special categories of cited documents:</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"Z" document member of the same patent family</p>		
Date of the actual completion of the international search 04 November 1998 (04.11.98)		Date of mailing of the international search report 03 November 1998 (03.11.98)
Name and mailing address of the ISA/ European Patent Office Facsimile No.		Authorized officer Telephone No.

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP 98/0212

A. KLASSTIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

H 04 Q 11/04

Nach der internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK6

B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfzettel (Klassifikationssystem und Klassifikationssymbole)

H 04 L, H 04 M, H 04 Q

Recherchierte aber nicht zum Mindestprüfzettel gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Bez. Anspruch Nr.
A	GB 2301264 A (MITSUBISHI DENKI KABUSHIKI KAISHA) 27. November 1996 (27.11.96). Zusammenfassung, Seite 1. Zeile 1 - Seite 10, Zeile 13. Fig. 5, Ansprüche 1,2. --	1
A	US 5369707 A (FOLLENDRE, III) 29. November 1994 (29.11.94). Zusammenfassung, Spalte 1. Zeile 5 - Spalte 4, Zeile 15. Fig. 4, Anspruch 1. --	1
A	US 5548635 A (BRADLEY et al.) 20. August 1996 (20.08.96). -----	

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☐ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen:

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis der der Erfindung zugrundeliegenden Prinzipien oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung, die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderscher Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung, die beanspruchte Erfindung kann nicht als auf erfinderscher Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"Z" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

04 November 1998

Abschließdatum des internationalen Recherchenberichts

03.11.98

Name und Postanschrift der internationalen Recherchenbehörde

Europäisches Patentamt, P.O. 5812 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Bevollmächtigter Beauftragter

GRÖSSING e.h.

ANHANG

zum internationalen Recherchen-
bericht über die internationale
Patentanmeldung Nr.

ANNEX

to the International Search
Report to the International Patent
Application No.

ANNEXE

au rapport de recherche inter-
national relatif à la demande de brevet
international n°

PCT/EP 98/02121 SAE 196651

In diesem Anhang sind die Mitglieder
der Patentfamilien der im obenge-
nannten internationalen Recherchenbericht
angeführten Patentdokumente angegeben.
Diese Angaben dienen nur zur Unter-
richtung und erfolgen ohne Gewähr.

This Annex lists the patent family
members relating to the patent documents
cited in the above-mentioned inter-
national search report. The Office is
in no way liable for these particulars
which are given merely for the purpose
of information.

La présente annexe indique les
membres de la famille de brevets
relatifs aux documents de brevets cités
dans le rapport de recherche inter-
national visée ci-dessus. Les renseigne-
ments fournis sont donnés à titre indica-
tif et n'engagent pas la responsabilité
de l'Office.

Im Recherchenbericht angeführtes Patentdokument Patent document cited in search report Document de brevet cité dans le rapport de recherche	Datum der Veröffentlichung Publication date Date de publication	Mitglied(er) der Patentfamilie Patent family member(s) Membres(s) de la famille de brevets	Datum der Veröffentlichung Publication date Date de publication
GB A1 2301264	27-11-96	GB A0 9510799	19-07-95
US A 5369707	29-11-94	CA AA 2101196	28-07-94
US A 5548635	20-08-96	CA AA 2133950	22-07-95

BEST AVAILABLE COPY

THIS PAGE BLANK (USPTO)